Espacenet

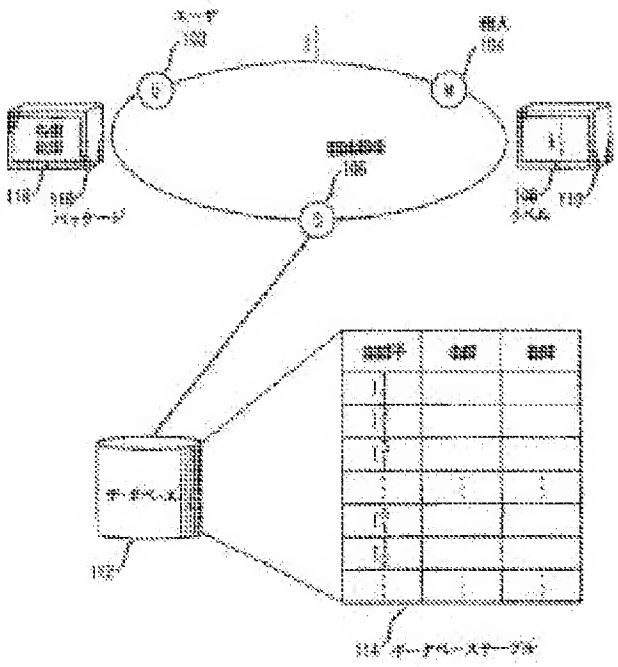
Bibliographic data: JP2001312680 (A) — 2001-11-09

METHOD FOR ELECTRONIC COMMERCE AND DATA BASE

Inventor(s):	JAKOBSSON BJORN M; REITER MICHAEL KENDRICK; SILBERSCHATZ ABRAHAM ±
Applicant(s):	LUCENT TECHNOLOGIES INC ±
Classification:	**- international:** ***G06Q10/00; G06Q30/00;*** (IPC1-7): G06F17/60 **- European:** G06Q10/08; G06Q30/04
Application number:	JP20010122699 20010420
Priority number (s):	US20000561535 20000428
Also published as:	EP1150227 (A1) CA2339560 (A1)

Abstract of JP2001312680 (A)

PROBLEM TO BE SOLVED: To provide an anonymous delivery method which cannot be linked in electronic commerce. SOLUTION: The anonymous delivery/payment method used in connection with electronic commerce is provided. A user starts electronic transaction with a merchant and therefore a specific identifier is supplied to the merchant. For starting respective transactions by the user, the specific identifier supplied to various traders is changed. The merchant attaches the identifier to a label on a package including the commodity which is to be delivered to the user by the reception of the identifier and the package is supplied to the delivery agent being a third person to whom the package is entrusted. The delivery agent accesses a data base for relating the identifier to the address of the specified user. The delivery agent exchanges the label for the label including the name and



the address of the user and delivers the package to the user.

Last updated: 14.03.2012 Worldwide Database 5.7.38; 92p

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－312680
（P2001－312680A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	４２４	Ｇ０６Ｆ　17/60	４２４
	３１０		３１０Ｅ
	３３４		３３４
	４３０		４３０
	ＺＥＣ		ＺＥＣ

審査請求　未請求　請求項の数40　ＯＬ　（全 14 頁）

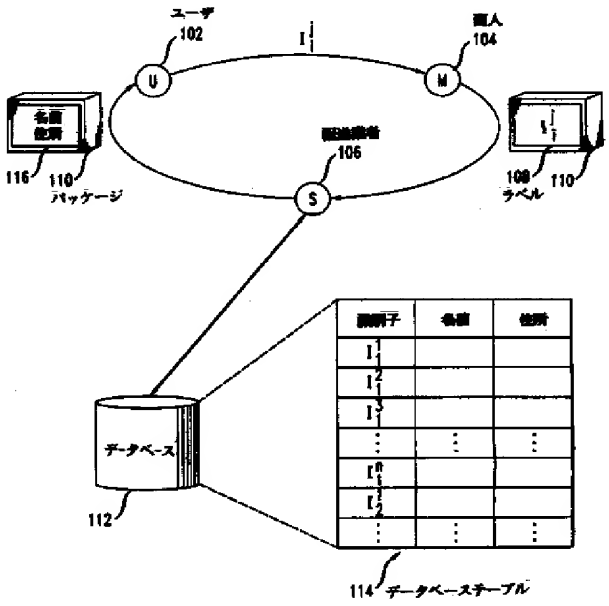
(21)出願番号　特願2001－122699(P2001－122699)
(22)出願日　平成13年４月20日(2001.4.20)
(31)優先権主張番号　０９／５６１５３５
(32)優先日　平成12年４月28日(2000.4.28)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　596077259
ルーセント　テクノロジーズ　インコーポレイテッド
Ｌｕｃｅｎｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
アメリカ合衆国　07974　ニュージャージー、マレーヒル、マウンテン　アベニュー　600－700
(74)代理人　100081053
弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】　電子商取引のための方法およびシステムおよびデータベース

(57)【要約】
【課題】　エレクトロニックコマースにおけるリンク可能でない匿名性配達技法を提供すること。
【解決手段】　エレクトロニックコマースとの関連で使用するための匿名の配達および支払い技法である。ユーザは、商人との電子的取引に入ることにより、固有の識別子を商人に提供する。このユーザにより各取引に入るために、様々な商人に提供される固有の識別子は変化する。識別子の受け取りにより、商人は、その識別子をユーザに配達されるべき商品を含むパッケージ上のラベルに付け、このパッケージを委託された第三者の配送業者に提供する。配送業者は、識別子を特定のユーザの住所に関連づけるために、データベースにアクセスする。その後、配送業者は、そのラベルを、ユーザの名前および住所を含むラベルと取り替え、そのパッケージをユーザに配達する。



【特許請求の範囲】
【請求項１】　商人から識別子を受け取るステップと、
前記受け取られた識別子に基づいて複数のユーザのうちの１つを同定するステップと、
前記一人のユーザの住所を決定するステップとを有し、
前記複数のユーザの各々は、少なくとも２つの異なる受け取られた識別子に基づいて、同定され得ることを特徴とする方法。
【請求項２】　パッケージを前記決定されたアドレスにおける前記一人のユーザに配送するステップをさらに含むことを特徴とする請求項１記載の方法。
【請求項３】　前記同定するステップは、
前記受け取られた識別子を使用してデータベースルックアップを実行するステップを含むことを特徴とする請求項１記載の方法。
【請求項４】　前記データベースルックアップで、前記一人のユーザを同定することができなかった場合、
少なくとも１つの識別子を生成し、
前記生成された識別子を前記受け取られた識別子と比較するステップをさらに含むことを特徴とする請求項３記載の方法。
【請求項５】　前記少なくとも１つの識別子を生成するステップは、
前記データベースに記憶された情報を使用して前記少なくとも１つの識別子を生成するステップを含むことを特徴とする請求項４記載の方法。
【請求項６】　前記少なくとも１つの識別子を生成するステップは、
前記商人から受け取られた追加的情報を使用して、前記少なくとも１つの識別子を生成するステップを含むことを特徴とする請求項５記載の方法。
【請求項７】　前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項６記載の方法。
【請求項８】　前記カウンターは暗号化されていることを特徴とする請求項７記載の方法。
【請求項９】　前記識別子は、前記商人からパッケージラベル上で受け取られることを特徴とする請求項１記載の方法。
【請求項１０】　前記受け取られた識別子は、記憶された値の第１の部分であり、前記方法は、
前記商人からメッセージおよび第１の暗号化されたメッセージを受け取るステップと、
前記記憶された値の第２の部分を検索するステップと、
第２の暗号化されたメッセージを生成するために、前記値の前記第２の部分を使用して前記受け取られたメッセージを暗号化するステップと、
前記第１の暗号化されたメッセージが、第２の暗号化されたメッセージと一致するかどうかを決定するステップをさらに含むことを特徴とする請求項１記載の方法。
【請求項１１】　前記第１の暗号化されたメッセージが、前記第２の暗号化されたメッセージと一致する場合、前記受け取られたメッセージを有効化するステップをさらに含むことを特徴とする請求項１０記載の方法。
【請求項１２】　前記メッセージは、金額を示すことを特徴とする請求項１１記載の方法。
【請求項１３】　前記同定するステップは、
前記データベースに記憶された情報を使用して少なくとも１つの識別子を生成するステップを含むことを特徴とする請求項１記載の方法。
【請求項１４】　前記少なくとも１つの識別子を生成するステップは、
前記商人から受け取られた追加的情報を使用して、前記少なくとも１つの識別子を生成するステップを含むことを特徴とする請求項１３記載の方法。
【請求項１５】　前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項１４記載の方法。
【請求項１６】　前記商人から受け取られた前記追加的情報は、ランダム数を含むことを特徴とする請求項１４記載の方法。
【請求項１７】　商人から受け取られた識別子を読み取るための手段と、前記受け取られた識別子に基づいて複数のユーザのうちの一人を同定するための手段と、
前記一人のユーザの住所を決定するための手段とを有し、
前記複数のユーザの各々は、少なくとも２つの異なる受け取られた識別子に基づいて同定され得ることを特徴とするシステム。
【請求項１８】　前記識別子を読み取るための手段は、バーコードスキャナであることを特徴とする請求項１７記載のシステム。
【請求項１９】　前記同定するための手段は、
前記受け取られた識別子を使用してデータベースルックアップを実行するための手段を含むことを特徴とする請求項１７記載のシステム。
【請求項２０】　前記データベースルックアップが失敗した場合に使用するために、
少なくとも１つの識別子を生成するための手段と、
前記受け取られた識別子と前記生成された識別子を比較するための手段とをさらに含むことを特徴とする請求項１９記載のシステム。
【請求項２１】　前記少なくとも１つの識別子を生成するための手段は、
前記データベース中に記憶された情報を使用して前記少なくとも１つの識別子を生成するための手段を含むことを特徴とする請求項２０記載のシステム。
【請求項２２】　前記少なくとも１つの識別子を生成するための手段は、
前記商人から受け取られた追加的情報を使用して前記少

なくとも１つの識別子を生成するための手段をさらに含むことを特徴とする請求項２１記載のシステム。
【請求項２３】　前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項２２記載のシステム。
【請求項２４】　前記カウンターは暗号化されていることを特徴とする請求項２３記載のシステム。
【請求項２５】　前記識別子は、前記商人から、パッケージラベル上で受け取られることを特徴とする請求項１７記載のシステム。
【請求項２６】　前記受け取られた識別子は、記憶された値の第１の部分であり、前記システムは、
前記商人からメッセージおよび第１の暗号化されたメッセージを受け取るための手段と、
前記記憶された値の第２の部分を検索するための手段と、
第２の暗号化されたメッセージを生成するために、前記値の前記第２の部分を使用して、前記受け取られたメッセージを暗号化するための手段と、
前記第１の暗号化されたメッセージが、前記第２の暗号化されたメッセージと一致するかどうかを決定するための手段とをさらに含むことを特徴とする請求項１７記載のシステム。
【請求項２７】　前記第１の暗号化されたメセージが、前記第２の暗号化されたメッセージに一致する場合、前記受け取られたメッセージを有効化するための手段をさらに含むことを特徴とする請求項２６記載のシステム。
【請求項２８】　前記メッセージが、金額を示すことを特徴とする請求項２７記載のシステム。
【請求項２９】　前記同定するための手段は、
前記データベース中に記憶された情報を使用して、少なくとも１つの識別子を生成するための手段を含むことを特徴とする請求項１７記載のシステム。
【請求項３０】　前記少なくとも１つの識別子を生成するための手段は、
前記商人から受け取られた追加的情報を使用して、前記少なくとも１つの識別子を生成するための手段を含むことを特徴とする請求項２９記載のシステム。
【請求項３１】　前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項３０記載のシステム。
【請求項３２】　前記商人から受け取られた前記追加的情報は、ランダム数を含むことを特徴とする請求項３０記載のシステム。
【請求項３３】　受け取られた識別子を住所と関連づけるために配送業者により使用するためのデータベースであって、各々がデータを記憶するための複数のフィールドを含む複数の記録を含み、前記記録の各々が、少なくとも、
１つの固有の識別子および１つの住所を記憶し、
少なくとも２つの記録が、異なる固有の識別子および同じ住所を含むことを特徴とするデータベース。
【請求項３４】　前記記録の各々が、少なくとも、
１つのカウンターおよび１つのキーを記憶し、
前記固有の識別子は、前記カウンターおよび前記キーの関数であることを特徴とする請求項３３記載のデータベース。
【請求項３５】　前記固有の識別子は、第１の部分および第２の部分を含むことを特徴とする請求項３３記載のデータベース。
【請求項３６】　受け取られた識別子と住所とを関連づけるために、配送業者により使用するためのデータベースであって、各々が、データを記憶するための複数のフィールドを含む複数の記録を含み、前記記録の各々は、少なくとも、
１つの固有の識別子、
１つのカウンター、
１つのキー、および
１つの住所を記憶し、
前記固有の識別子は、前記カウンターおよび前記キーの関数であることを特徴とするデータベース。
【請求項３７】　特定のアドレスは、１つのデータベース記録中にのみあることを特徴とする請求項３６記載のデータベース。
【請求項３８】　受け取られた識別子が、前記データベース記録のうちの１つ中に記憶された固有の識別子と一致する場合、
前記１つのデータベース記録中の前記カウンターは、インクリメントされ、
前記１つのデータベース記録中の前記固有の識別子は、更新されることを特徴とする請求項３７記載のデータベース。
【請求項３９】　特定の住所は、少なくとも２つのデータベース記録中にあることを特徴とする請求項３６記載のデータベース。
【請求項４０】　前記識別子は、第１の部分および第２の部分を含むことを特徴とする請求項３６記載のデータベース。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、エレクトロニックコマースに係り、特に、データネットワークを介して注文された商品の匿名のかつ安全な配達および支払いに関する。
【０００２】
【従来の技術】電子商取引の数が増大しているので、プライバシーがますます重要になってきている。オンライン購入のトラッキングおよびプロファイリングの可能性のために、エレクトロニックコマースに関わることをためらう購入者がいる。そして、これらの購入者は、伝統

的な、特に現金の取引により提供される匿名性のために、従来の“brick and mortar”ビジネスを好む。

【０００３】オンライン取引において匿名性を提供するための主要な障害は、オンラインで購入される商品が、購入者に物理的に配達されなければならないという電子的取引のまさに性質から生じる。勿論、これは、商品が配送され得るように、購入者が商人（merchant)に彼の／彼女の名前および住所を提供することを必要とする。商人は、購入情報を集め、これを、マスメーリング（mass mailings）のようなマーケティング目的のために使用する。この匿名性の問題は、エレクトロニックコマース産業に対する主要な障害である。

【０００４】１つの解決法は、米国特許第６，００６，２００（”Boies et al.”）に示されており、ここでは、顧客の名前および住所情報が、配送業者のような信頼おける第三者のデータベースに預けられる。各顧客は、顧客の名前および住所に関連づけられたデータベース中に記憶された固有の識別子を受け取る。データベースエントリがセットアップされた後、顧客は、オンライン購入を行い、商人に固有の識別子のみを提供することができる。商人は、購入されたアイテムを含む物理的パッケージ上にその固有の識別子を付け、パッケージを委託された第三者の配送業者に提供する。そして、配送業者は、その固有の識別子に基づいて顧客の名前および住所を決定し、そのパッケージを顧客に配達する。

【０００５】Boies 等による特許に示された技法は、あるレベルの匿名性を提供するが、この提案された解決法にはいくつもの問題がある。第１に、そのスキームを使用するシステムにおける取引は、いわゆるリンク可能であり、一人または二人以上の商人は、購入情報をある期間について集めることができ、その集められた購入情報は、特定の識別子に関連づけられた購入者についての所定の情報が発見され得るように相関づけられ得る。期間が長く取引の回数が多い場合、特定の固有の識別子に関連づけられた購入者の名前および住所さえも、ある程度の正確さで決定され得る。

【０００６】Boies 等による技法についての別の問題は、購入されたアイテムについての支払いを考慮に入れてないことである。配達メカニズムがある程度匿名であったとしても、購入に対する支払いは、別の問題および別の匿名性の欠如を提供する。ほとんどのオンライン購入は、クレジットカードを使用してなされるので、商人は、注文を処理するために、購入者の名前および住所を知らなければならない。勿論、Boies 等の特許において解決されていないが、匿名の支払いは、別の委託された第三者によりアレンジされ得る。しかし、そのような委託された第三者、購入者および商人の組合せを調整することは、ロジスティック的に困難である。

【０００７】

【発明が解決しようとする課題】エレクトロニックコマース産業を刺激するために必要とされているものは、リンク可能でない匿名性配達技法である。そのような配達技法が、購入者が匿名のままであることを可能にする改良された支払いスキームと組み合わされ得る場合、更なる利益が得られる。

【０００８】

【課題を解決するための手段】ユーザが商人から配送されるべき商品を購入するとき、ユーザは、商人に固有の識別子を提供する。その後、その商人は、商品を含むパッケージを、固有の識別子をユーザと関連づけることができる委託された第三者の配送業者に提供する。本発明によれば、そして従来技術と異なり、特定のユーザにより一人または二人以上の商人に提供される連続的な固有の識別子は、一連の取引の各々の間に変化する。

【０００９】結果として、本発明の利点によれば、例え長い期間について集められた多数の識別子の知識があっても、購入者およびその購入についてのいかなる有用な情報も提供しないことになる。各ユーザが複数の取引について同じ識別子を使用する従来技術による技法は、取引をリンク可能にしたが、複数の取引について異なる識別子を使用する本発明の技法は、取引をリンク不可能にする。

【００１０】本発明の一実施形態によれば、商人は、ユーザから受け取った固有の識別子をパッケージラベルに付け、そのパッケージを第三者の委託された配送業者に提供し、その配送業者は、その固有の識別子をユーザと関連づけ、そのパッケージをユーザの住所に配達する。配送業者は、以前の登録プロセスの間に、既に複数の固有の識別子を特定のユーザに関連づけた。この事前の関連づけは、様々なやり方で行われ得る。

【００１１】一実施形態において、配送業者は、複数の固有の識別子を生成し、これらの識別子をユーザに提供する。ユーザおよび配送業者の双方が、これらの識別子をコンピュータメモリ中に記憶する。その後、オンライン取引において、ユーザは、これらの識別子のうちの１つを商人に提供する。配送業者がラベル上に１つの識別子を有するパッケージを受け取るとき、配送業者は、受け取った識別子を見つけ、関連づけられたユーザの住所を決定するために、データベースルックアップを実行する。

【００１２】別の実施形態によれば、ユーザおよび配送業者は、ユーザと配送業者との間で交換された既知のパラメータの値に基づいて、ダイナミックに識別子を生成することができる。特定の実施形態によれば、これらのパラメータは、連続的なオンライン取引の間、既知のインクリメントアルゴリズムによりインクリメントされるカウンターと共に、各ユーザに割り当てられた固有のキーである。各取引の後にカウンターは変化するので、連続的取引に関して商人により受け取られる識別子は、異なり、商人によりリンク不可能である。別の特定の実施

形態において、これらのパラメータは、ユーザにより生成されたランダム数を伴う固有のキーである。

【００１３】以下にさらに詳細に説明する可能性のあるカウンター同期化エラーのために、配送業者は、各ユーザに対して、一連の固有の識別子を含む複数の記録を記憶することができる。これは、所定レベルの同期化エラーが存在したとしても、この技法が正しく動作することを可能にする。さらに別の技法によれば、同期化エラーが所定レベルを超えたとしても、ある識別子を適切なユーザと関連づけることは、外挿法の使用により実行され得る。新しい固有な識別子は、配送業者のデータベース情報のみを使用して、または配送業者に提供される追加の情報とも組合せで外挿され得る。

【００１４】本発明の別の実施形態によれば、匿名の支払い技法は、上述した匿名の配達技法と組み合わされる。この実施形態によれば、配送業者は、商品について商人に支払い、ユーザは、商品について支払われた額、配送料、および任意的な取引処理料を配送業者に支払う。配送業者は、ユーザから商人に送られ、商人から配送業者に転送されたメッセージおよび暗号化されたメッセージを使用して、商品についての支払いに対するユーザの同意を認証する。

【００１５】購入価格の認証により、配送業者は、ユーザが、配達される商品について特定の価格を支払うことを同意したことを確かにすることができる。そして、配送業者は、商品について認証された額を商人に支払うことができ、配送業者は、ユーザがその商品について認証された額を支払うことを同意したことを確かにすることができる。

【００１６】

【発明の実施の形態】本発明の一実施形態を、図１を参照して説明する。図１は、ユーザＵ１０２、商人Ｍ１０４、および配送業者Ｓ１０６を含む。最初に、ユーザ１０２および商人１０４は、通信し、ユーザ１０２が商人１０４から商品を購入するということを合意する。この通信は、典型的には、データネットワーク（例えば、インタネット）を介して通信するユーザコンピュータと商人コンピュータによる。この時点において、我々は、商品についての支払いの問題を無視する。匿名の支払いを付け加える技法は、後述する。

【００１７】販売の条件が合意されると、ユーザ１０２は、識別子I_i^jを商人１０４に送る。本発明の一側面によれば、そして従来技術と異なり、ユーザから商人に送られる識別子は、各取引で変化する。そして、I_i^jの表記は、ｉ番目のユーザのｊ番目の識別子を意味する。したがって、一連の取引の各々に対して、ｉ番目のユーザは、一連の識別子I_i^1，I_i^2，I_i^3，…，I_i^nのうちの１つを送ることになる。そして、商人との最初の取引について、ｉ番目のユーザは、識別子I_i^1を商人に送ることになる。

【００１８】その後、同じユーザと同じまたは異なる商人との間の次の取引について、そのユーザは、識別子I_i^2を送ることになる。識別子は各取引で変化するので、長い期間について多数の取引に関する情報を有したとしても、商人は購入者についてのいかなる情報も見つけることは不可能である。そして、本発明は、上述したリンク可能性の問題を実質的に減少させる。

【００１９】図１において、識別子I_i^jの受け取りにより、商人１０４は、その識別子を、その取引の間に、ユーザ１０２により注文された商品を含むパッケージ１１０のラベル１０８に付ける。この時点において、商人１０４は、ユーザ１０２のアイデンティティもユーザ１０２の住所も知らない。商人１０４は、この取引についてのユーザの識別子がI_i^jであることを知り、配送業者１０６がパッケージ１１０をユーザ１０２に適切に配達できるように、ユーザ１０２が配送業者１０６と関係を有していることを知る。そして、商人１０４は、パッケージ１１０を配送業者１０６へ提供する。

【００２０】パッケージ１１０の受け取りにより、配送業者１０６は、識別子I_i^jを決定するために、ラベル１０８を読み取る。ラベル１０８は、望ましくは、配送業者がラベルの読み取りを自動化できるように、機械読み取り可能なフォーマットになっていることに留意すべきである。勿論、ラベルの特定の機械読み取り可能なフォーマットは、識別子をラベル１０８に付ける際に商人１０４により使用される技法および識別子をラベルから読み取る際に配送業者１０６により使用される技法の両方を決定することになる。

【００２１】一例として、商人は、バーコードスキャナを使用して配送業者により読み取り可能なバーコードラベルを印刷することができる。配送業者１０６が識別子I_i^jを読み取ると、配送業者１０６は、識別子とユーザの名前および住所との間の関連を記憶するデータベーステーブル１１４を含むデータベース１１２にアクセスする。図１に示されているように、テーブルは、各ユーザに対して複数の識別子を記憶する。例えば、ユーザ１に対して、テーブル１１４は、ｎ個の識別子を記憶するように示されている。

【００２２】配送業者１０６は、商人１０４から受け取ったパッケージ１１０について、ラベル１０８から読みとった識別子に関連づけられた名前および住所を決定するために、データベースルックアップを実行する。これらの識別子は、各識別子が１つのデータベース記録を独特に同定し、重複の可能性が極めて小さく、かつ存在しないと思われるということを保証するために十分に大きいように設計される。識別子の生成は、後述する。

【００２３】受け取った識別子と一致する適切なデータベース記録を配送業者１０６が見つけると、配送業者１０６は、名前および住所のラベル１１６をパッケージ１１０に付け、パッケージ１１０はユーザ１０２に配送す

ることになる。そして、このようにして、ユーザ１０２は、商人１０４から商品を匿名に受け取る。委託された第三者である配送業者１０６のみが、識別子ユーザの名前および住所と相関させることができる。

【００２４】上述したように、従来技術による匿名の配達方法にないこの技法の利点は、連続するオンライン取引の各々について異なる固有の識別子をユーザが使用するので、本発明による技法は、リンク可能でないことである。即ち、商人が取引情報を集めることができたとしても、そのような情報は、何れか一人の特定のユーザにリンクさせることは困難である。

【００２５】ここに示されたステップは、配送業者により、プログラム可能なコンピュータを使用して、望ましくは実行され得ることに留意すべきである。そのようなコンピュータは、プロセッサによりアクセス可能なメモリ中に記憶されたコンピュータプログラムコードを実行するためのプロセッサを含む。ここで使用されているように、メモリの用語は、これに限定されるものでないが、ランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、磁気ディスク、光ディスク、およびホログラフィックメモリを含む何れかのコンピュータで読み出し可能な媒体を指すために使用される。

【００２６】望ましい実施形態において、コンピュータプログラムコードは、コンピュータプロセッサに接続されたＲＡＭのような高速メモリに記憶される。本発明を実施するために必要とされるコンピュータプログラムコードは、何れかの周知のコンピュータ言語で書くことができる。本発明のこの説明により、当業者は、本発明を実施するために必要なプログラムコードを容易に書くことができる。

【００２７】また、コンピュータは、周知の方法で、データベース１１２と通信することになる。ユーザは、周知の入出力装置および技法（例えば、ディスプレイスクリーン、キーボード、マウス）を使用してコンピュータと相互作用する。ここに説明されたタイプのプログラム可能なコンピュータは、この技術分野においてよく知られており、さらに説明する必要のないものである。

【００２８】上述したスキームを正しく働かせるために、ユーザ１０２により使用される特定の識別子I_i^jは、データベース１１４においてユーザの名前および住所と事前に関連づけられなければならない。この事前の関連づけを実行するために、様々な技法がある。

【００２９】第１の実施形態において、特定のユーザにより使用されるべき識別子は、配送業者により前もって生成され、ユーザのコンピュータに記憶するためにユーザに提供される。例えば、ユーザ１０２が、ここで説明される匿名の配達サービスに加入することを望む場合、ユーザは配送業者１０６に登録し、一連の識別子を要求する。配送業者１０６は、ｎ個のそのような識別子を生成し、これらのｎ個の識別子をユーザに提供する。

【００３０】配送業者は、これらのｎ個の識別子をそのデータベーステーブル１１４に記憶する。そして、ｉ番目のユーザに対して生成されるｎ個の識別子は、I_i^1，I_i^2，I_i^3，…，I_i^nとなる。これらの同じｎ個の識別子I_i^1，I_i^2，I_i^3，…，I_i^nは、ユーザｉのコンピュータにも記憶されることになる。この実施形態によれば、配送業者が商人から識別子I_i^jを受け取るとき、配送業者は、配送のための名前および住所を決定するために、その識別子を含む固有の記録を探す。

【００３１】ある識別子が使用された後、それは、ユーザのコンピュータおよび配送業者のデータベース１１２の両方の記憶から削除され得る。これは、上述したように、各固有の識別子が、一度だけ使用されるからである。この実施形態は、ユーザのコンピュータおよび配送業者のデータベースの両方において多量の記憶を必要とすることが認識される。これは、特に、固有の識別子I_i^jが、重複がないことを保証するためにかなり多数でなければならないという事実による。

【００３２】本発明の別の実施形態によれば、ユーザおよび配送業者は、必要な場合に、ダイナミックに識別子を生成する。この実施形態において、ユーザが、サービスに対する加入者として配送業者に登録するとき、配送業者は、ユーザに対して固有のキーを提供する。ｉ番目のユーザに対して、我々は、このキーをK_iと呼ぶ。配送業者は、ユーザに、カウンターについての初期値を提供する。ｉ番目のユーザに対して、我々は、このカウンターをC_iと呼ぶ。

【００３３】カウンターは、ユーザおよび配送業者の両方に知られた何らかの既知のインクリメントアルゴリズムに従って、増加的に変化することになる。例えば、このアルゴリズムは、C_iからC_i+sへの単なる値の変化であり得る。ここで、ｓは正または負の整数である。勿論、インクリメントアルゴリズムは、配送業者およびユーザの両方に知られたいかなるアルゴリズムであってもよい。

【００３４】単純な表記として我々は、そのインクリメントアルゴリズムに従って一度インクリメントされたカウンターC_iを指すために、表記C_i+1を使用する。この実施形態によれば、識別子I_i^jは、ユーザおよび配送業者が、K_iおよびC_iの知識を使用してI_i^jをダイナミックに生成できるように、K_iおよびC_iの一方向関数（one-way function）として演算される。この関数は、K_iおよびC_iがI_i^jの知識から決定され得ないという点で、一方向である。

【００３５】この実施形態は、図２との関連で説明される。この実施形態において、ユーザ２０２が、商人２０４との取引に関わるとき、ユーザ２０２は、ユーザのコンピュータに記憶されたK_iおよびC_iの値に基づいて、I_i^jをダイナミックに生成し、この識別子I_i^jを商人２０４へ送る。ユーザは、次の取引において、ユーザが異

なるI_i^jを生成することになるように、インクリメントアルゴリズムに基づいて、C_iの値をC_i+1へインクリメントする。配送業者の側で、配送業者２０６が、商人２０４から、ラベル２０８上に識別子I_i^jを含むパッケージ２１０を受け取るとき、配送業者２０６は、上述したように、一致する識別子を含む記録について、そのデータベース２１２をサーチする。

【００３６】この実施形態によれば、配送業者のデータベース２１２は、図２に示されたデータベーステーブル２１４を記憶する。各ユーザｉについて、データベーステーブル２１４は、カウンターC_iの現在の値を使用して生成された固有の識別子I_i^j、ユーザの名前および住所、カウンターC_iの現在の値、インクリメントアルゴリズム、およびユーザのキーK_iを記憶する記録を含む。

【００３７】配送業者２０６がラベル２０８上で受け取られた識別子I_i^jをデータベーステーブル２１４中に見つけるとき、配送業者は、その識別子に関連づけられた名前および住所を有するラベル２１６を印刷し、そのパッケージ２１０をユーザに配送する。この実施形態において、配送業者は、ユーザについてのデータベース記録を、以下のように更新する。配送業者は、インクリメントアルゴリズムに従って、記録中のC_iの値をインクリメントする。

【００３８】そして、配送業者は、K_iおよび更新されたC_iの値に基づいて新しい識別子I_i^jを演算する。そして、この実施形態において、上述した実施形態の記憶の問題は、解決される。これは、ユーザおよび配送業者が、多数の事前に演算された識別子を記憶するのではなく、固有の識別子をダイナミックに生成するために必要とされる情報をユーザおよび配送業者が記憶するからである。

【００３９】識別子がダイナミックに生成される上述した実施形態の１つの可能性のある問題は、ユーザおよび配送業者が、適切な同期を保たなければならないことである。即ち、ユーザおよび配送業者により保持されるカウンターC_iの値は、同じでなければならない。さもなければ、ダイナミックに生成される識別子は、一致しないことになる。同期化の問題を解決するためのいくつかの方法がある。まず、ユーザが識別子I_i^jを商人に送る状況を考える。

【００４０】そして、ユーザは、上述した技法に従って、そのカウンターC_iをインクリメントする。しかし、商人がそのラベル上に識別子I_i^jを有するパッケージを送ることに先立って、商人のコンピュータが、クラッシュし、そして商人が、取引に関する情報を失い、配送業者が、商人から識別子I_i^jを受信しない。そして、配送業者は、この特定のユーザに関連づけられたカウンターC_iをインクリメントすることがなく、ユーザのカウンターC_iおよび関連づけられた配送業者のカウンターC_iが、同期外れになっている。

【００４１】このユーザの次の取引において、ユーザは、インクリメントされたカウンター（即ち、C_i+1のカウンター値）に基づいて次の識別子を生成することになるが、その識別子の受け取りにより、配送業者は、そのデータベース中にその識別子を言い出すことができなくなる。これは、そのユーザに対する記録が、C_iのインクリメントされていないカウンター値を使用して生成された識別子を含むからである。

【００４２】ユーザおよび配送業者を同期外れにする別のやり方は、以下の通りである。ユーザが第１の商人との取引に入り、識別子I_i^jをその商人に送ることを考える。そして、ユーザは、上述した技法に従ってそのカウンターC_iをインクリメントする。ユーザは、第２の商人との別の取引に入り、インクリメントされたカウンター値C_i+1に基づいて、次の識別子I_i^{j+1}を第２の商人に送る。しかし、第２の商人のパッケージは、配送業者に最初に到着し、配送業者は、識別子I_i^jを受け取る前に識別子I_i^{j+1}を受け取る。この時点において、このユーザに対する配送業者のデータベース記録は、識別子I_i^jを含んだままである。したがって、このシステムは、同期外れとなり、適切に動作しないことになる。

【００４３】同期外れ問題の１つの解決法は、図３に示されたようなデータベース３０２を構成しかつ保持することである。この実施形態において、一連の識別子が、各ユーザに対して記憶される。テーブル３０２は、ｉ番目のユーザに対する記憶された記録を示す。テーブル３０２は、識別子I_i^1，I_i^2，I_i^3，…I_i^nを含むｎ個の記録を記憶する。これらの識別子は、ｉ番目のユーザのキーK_iおよびｉ番目のユーザのカウンターC_iの$C_i+(n-1)$への増分値を使用して生成される。

【００４４】そして、配送業者が、（カウンター値に基づいて）期待された特定の順序で識別子を受け取らない場合であっても、配送業者は、テーブル３０２中のマッチング記録を受信された識別子に恐らく一致させることになる。ｎの値は、配送業者のデータベースの記憶容量と配送業者が取り扱うことを望む非同期の程度のバランスとして選択され得る。

【００４５】別の技法によれば、ユーザおよび配送業者が値ｎより大きい量だけ同期外れになったとしても、配送業者は、それにも関わらず、以下のように識別子を取り扱うことができる。図３に示された実施形態において、配送業者が、データベーステーブル３０２中に存在しない識別子を含むパッケージを受け取ったと考える。配送業者は、その時点において、識別子が無効であり、パッケージの処理を終了させることを仮定することができる。

【００４６】しかし、配送業者は、以下のように、パッケージに関連づけられたユーザを決定することを試みるために、データベーステーブル３０２中の存在するデー

タを外挿することを試みることができる。配送業者は、データベーステーブル３０２において、ユーザの各々に対する連続するｘ個の識別子を計算することを試みることになる。例えば、ｘ＝３である場合、図３に示されたｉ番目のユーザに関して、配送業者は、そのユーザに対して最後に記憶された識別子の直後に続くシーケンス中の３個の識別子を計算することになる。

【００４７】したがって、図３に示された実施形態において、配送業者は、各ユーザに対してｎ個の記録を記憶し、ｉ番目のユーザに対する最後の記録は、I_i^nであり、配送業者は、それぞれC_i＋ｎ，C_iｎ＋１，C_i＋ｎ＋２ の増分カウンター値を使用してI_i^{n+1}，I_i^{n+2}，I_i^{n+3}をダイナミックに計算することになる。この外挿は、図３において３０６として示されているように、配送業者が別のｘ個のデータベーステーブル記録を生成することと考えられ得る。配送業者は、新たに生成された識別子のうちの１つが受信された識別子と一致するまで、または配送業者が、受け取った識別子がユーザに一致しないと決定するまで、ユーザの各々に対するこのｘ個の記録の外挿を実行することになる。

【００４８】上述した実施形態において、複数の記録が、各ユーザに対して記憶され、あるタイプのテーブルメンテナンスが、合理的なサイズ内にデータベーステーブルを保持するために実行されなければならない。例えば、配送業者が各ユーザに対して１０個の記録を記憶すると考えると、ｉ番目のユーザに対して、データベーステーブルは、以下の識別子を含む記録を有する。即ち、I_i^1，I_i^2，I_i^3，…I_i^{10} である。配送業者が、商人からのパケットラベル上に識別子I_i^8を受け取ったと考える。配送業者は、その識別子を、ｉ番目のユーザに一致させ、パッケージを上記したように、そのユーザに配送する。

【００４９】配送業者は、何らかの同期エラーが生じ、配送業者は、そのユーザとの関連で何らかのより速いシーケンス識別子を受け取ることには恐らくならないという仮定をなすことができる。そして、テーブルメンテナンス動作に従って、配送業者は、識別子I_i^1，I_i^2，I_i^3，…I_i^6を含む記録を削除することができる。これは、これらの識別子は、このユーザに関連して恐らく受信されないからである。識別子I_i^7を含む記録は、データベース中に残っており、更なる同期の問題のために、ユーザはその識別子を依然として使用することができる。

【００５０】更なる別の実施形態において、ユーザは、識別子I_i^jおよびその識別子を生成するために使用されたカウンターC_i の両方を商人に供給することができる。この実施形態は、配送業者が、以下のように、新しい識別子をより容易に外挿することを可能にする。配送業者が、この特定のユーザに対して記憶され、以下の識別子、即ちI_i^1，I_i^2，I_i^3，…I_i^{10} を含む１０個の記録を有すると仮定する。そして、ユーザおよび配送業者が、同期外れとなっており、ユーザが識別子I_i^{14} を商人に送るようになっていると仮定する。

【００５１】また、この実施形態によれば、ユーザは、商人にC_i＋１３ も送る。これは、識別子I_i^{14} を演算するために使用されたカウンター値である。図３において、識別子I_i^n が、カウンター値C_i＋（ｎ－１）を使用して生成されたことを思い出されたい。そして、商人は、パッケージ上に、I_i^{14} およびC_i＋１３ を含むラベルを付ける。このパッケージの受領により、配送業者が、データベースルックアップを実行するが、識別子I_i^{14} を発見しない。

【００５２】上述した外挿技法に従って、配送業者は、ユーザの各々に対する新しい識別子を生成することを試みることができる。しかし、上述したように、外挿の数ｘ＝３である場合、このユーザに対して、配送業者は、I_i^{11}，I_i^{12}，I_i^{13} をダイナミックに生成し、受け取られた識別子I_i^{14} は、一致しないことになり、パッケージは配達されないことになる。

【００５３】しかし、この実施形態によれば、配送業者は、初期のデータベースルックアップを実行するが、識別子I_i^{14}を発見しない場合、配送業者は、この場合C_i＋１３であるラベル上のカウンター値を参照することになる。配送業者は、受け取られたカウンター値C_i＋１３ と共にユーザのキーを使用するシステムにおいて、ユーザの各々に対する識別子を生成することを試みることになる。そして、配送業者は、適切な識別子を生成し、データベース一致となるチャンスを改善しつつ、ユーザあたりの外挿を一度のみ必要とする。

【００５４】この技法の更なる改良において、配送業者は、速いデータベース一致の可能性を向上させるために、ユーザに対して特定の順序で識別子を外挿しかつ生成することができる。例えば、配送業者は、特定のユーザに対して最高のカウンター値が現在記憶されていることを知っているので、配送業者は、特定のユーザに対してデータベース中に記憶されたカウンター値の範囲が、商人から受け取ったカウンター値を既に超えている場合、この特定のユーザは問題となる識別子を生成したことは恐らくなく、配送業者は、このユーザをスキップし、識別子をダイナミックに生成しないと決定することができる。

【００５５】さらに別の性能改善によれば、配送業者は、最も可能性のあるユーザに対する識別子が最初に試みられるように外挿を命令するように試みることができる。例えば、特定のユーザがC_iないしC_i＋１０の範囲中のカウンター値を含む記憶された記録を有し、配送業者がカウンターC_i＋１１ をラベル上で受け取った場合、配送業者は、カウンターが１つのインクリメントにより同期外れとなっただけであるので、このユーザはたぶん外挿の候補であると判断することができる。

【００５６】上述した識別子と共にカウンターC_iをユーザが送る技法は、限定された数の場合において、商人が、所定の購入を特定のユーザと関連づけることを可能にすることに留意すべきである。例えば、商人がカウンターを受け取るので、商人は、これらのカウンターを集め、インクリメントアルゴリズムの何らかの決定を行い、何らかの取引間の相関をなすことができる。例えば、長い時間について、商人が、以下の識別子とカウンターとの組合せを受信したと仮定する。

【００５７】

TX ID	識別子	カウンター
1	123324384895	1
2	139483948395	129
3	957395739584	2
4	494958928923	55
5	957802852949	131
6	958395038503	88
7	472395023782	133
8	594848582385	3

【００５８】カウンターの分析により、商人は、取引識別子（ＴＸ　ＩＤ）１，３および８に同じユーザが関連づけられているという仮定を非常によく行うことができる。これは、$C_i = C_i + 1$のインクリメントアルゴリズムに関連づけられる取引のためのカウンターが、それぞれ１，２および３であるからである。同様に、商人は、同じユーザがＴＸ　ＩＤ２，５および７に関連づけられているという過程を行うこともできる。これは、$C_i = C_i + 2$のインクリメントアルゴリズムに関連づけられた取引のためのカウンターが、それぞれ１２９，１３１および１３３であるからである。勿論、これらの例は、商人により行われ得る分析の単純な例であるが、商人にカウンター値を提供することの可能性のある危険を示している。

【００５９】上述した相関を防止するために、本発明の別の実施形態によれば、ユーザは、識別子I_i^jおよびその識別子を生成するために使用されたカウンターC_iの暗号の両方を商人に供給する。望ましくは、配送業者は、周知の公開鍵／秘密鍵暗号化スキームに従って公開鍵／秘密鍵の対の公開鍵部分をユーザに提供する。ユーザは、公開鍵を使用してカウンターC_iを暗号化する。配送業者の公開鍵は、PK_sで表され、公開鍵PK_sを使用するカウンターC_iの暗号は、$E_{PKs}(C_i)$で表される。

【００６０】ユーザは、I_i^jおよび$E_{PKs}(C_i)$を商人に送る。そして、商人は、これらのパラメータを配送業者に送る。上述したものと同様に、配送業者は、そのデータベース中に一致する識別子I_i^jを有する記録を見つけることができない場合、カウンターを解読し、それを上述した新しい識別子を外挿するために使用することができる。しかし、この場合において、商人により受け取られたカウンターは暗号化されており、したがって、商人は、カウンターからいかなる有用な情報も発見することができない。

【００６１】$E_{PKs}(C_i)$は、かなり大きく、商人が、標準的配送ラベル上の暗号化されたカウンターを復号化することは困難であることに留意すべきである。そして、この実施形態の変形において、商人は、識別子I_i^jのみを配送ラベル上に付けることができる。配送業者が、そのデータベース中に一致する識別子を有する記録を発見できない場合にのみ、配送業者は、商人から関連づけられた$E_{PKs}(C_i)$を要求する。商人は、I_i^jおよび$E_{PKs}(C_i)$を含む別のラベルを送ることができるか、または$E_{PKs}(C_i)$は、商人から配送業者に電子的に送信され得る。

【００６２】我々は、ユーザおよび配送業者が、カウンターを使用することなしに、必要な場合に、識別子をダイナミックに生成する本発明の別の実施形態を説明する。図２との関連で上述したものと同様に、ｉ番目のユーザが、そのサービスに対する加入者として配送業者に登録している場合、配送業者は、ユーザに、固有のキーK_iを提供する。この固有のキーK_iは、ユーザおよび配送業者の両方に知られている。この実施形態における識別子I_i^jは、K_iの一方向関数および各取引についてユーザにより生成されるランダム数Ｒとして演算される。

【００６３】この実施形態は、図４との関連で説明される。ユーザ４０２が、商人４０４との取引に関わっているとき、ユーザ４０２は、K_iの値およびユーザ４０２により生成されるランダム数Ｒに基づいて、I_i^jをダイナミックに生成する。ユーザ４０２は、識別子I_i^jおよびランダム数Ｒを商人４０４へ送る。商人４０４は、パッケージ４１０のラベル４０８上へ、識別子I_i^jおよびランダム数Ｒを付け、そのパッケージを配送業者４０６へ提供する。

【００６４】この実施形態によれば、配送業者のデータベース４１２は、図4に示されたようなデータベーステーブル４１４を記憶する。各ユーザｉに対して、データベーステーブル４１４は、ユーザの名前および住所およびユーザのキーK_iを記憶する記録を含む。配送業者４０６はパッケージ４１０を受け取るとき、配送業者４０６は、ラベル４０８上の識別子I_i^jおよびランダム数Ｒを読み取る。そして、配送業者は、ユーザ４０２が受け取られた識別子を生成するために使用した同じ一方向関数と共に、受け取られたランダム数Ｒを使用して、データベーステーブル４１４中のキーK_iの各々を使用して新しい識別子を生成する。

【００６５】配送業者は、生成された識別子のうちの１つが受け取られた識別子と一致するまで識別子を生成し続ける。一致する識別子が生成されたとき、配送業者は、その一致する識別子を生成するために使用されたキーK_iが、そのパッケージに関連づけられたｉ番目のユ

ーザに属することを知り、配送業者は、テーブル４１４からｉ番目のユーザの関連する名前および住所を読み出すことができる。配送業者は、ユーザの名前および住所を有するラベルを印刷し、パッケージをユーザに配送する。

【００６６】この実施形態は、いくつかの場合において、カウンターを使用する上述した実施形態はより演算的に集約的であるが、この実施形態は、配送業者またはユーザがいかなる状態情報（例えば、カウンター値）を保存する必要がないので、カウンターの実施形態の同期の問題を解決する。また、この実施形態は、配送業者が、受信したランダム数を使用してユーザについてのいかなる情報も決定することを許容しない。

【００６７】ランダム数が、識別子のダイナミックな生成に使用される別の実施形態は、以下の通りである。この実施形態において、ユーザは、ランダム数Ｒに付加された彼／彼女の住所を暗号化することにより識別子を生成し、暗号化されたテキストを商人に送る。商人は、暗号化されたテキストをラベルに付け、パッケージを配送業者に提供する。パッケージの受け取りにより、配送業者は、暗号化されたテキストを読み取り、暗号化されたテキストを解読し、ユーザの名前および住所を抽出する。この実施形態において、配送業者は、暗号化されたテキストを解読するために使用され得るキーのみを記憶する必要がある。公開鍵／秘密鍵暗号化スキームを含む様々な周知の暗号化技法が、この実施形態に関連して使用され得る。

【００６８】図５を参照して、商人に対する金銭の支払いの認証について説明する。上述したように、匿名のエレクトロニックコマースについての問題の１つは、支払いがユーザから商人になされなければならないと言うことである。そのような支払いは、一般に、クレジットカードによりなされるので、商人が、支払いを処理するためにユーザの名前を知らなければならない。これは、匿名のエレクトロニックコマースの可能性を厳しく制限する。

【００６９】支払いが、別の委託された第三者を通してなされ得るが、そのような委託された第三者の支払いを受けるもの、委託された第三者の配送業者、購入者および商人の組合せを調整することはロジスティック的に困難である。そして、本発明の以下に説明する別の実施形態において、我々は、上述した匿名の配達技法との組合せで使用され得る改良された支払い技法を提供する。この実施形態によれば、商人は、配送業者から支払いを受け取り、配送業者は、ユーザからその支払額（任意の取引処理料をプラスして）取り戻すことができる。

【００７０】この実施形態において、識別子I_i^jは、上述したように、ユーザによりダイナミックに生成されるが、識別子は、２つの部分part１（I_i^j）およびpart２（I_i^j）に分けられる。例えば、I_i^jが３２ビットである場合、第１の１６ビットは、part１（I_i^j）となり、第２の１６ビットは、part２（I_i^j）となる。図５に示されているように、配送業者のデータベーステーブル５１４は、識別子のこれらの２つの部分を記憶する。ユーザ５０２は、電子的取引に関連づけられた支払い認証のために使用されるmessage を生成する。

【００７１】例えば、典型的なmessage は、「１００ドルを支払え」であり得る。そして、ユーザ５０２は、識別子の第２の部分を周知のメッセージ認証コード（ＭＡＣ）キーとして使用する一方で、ＭＡＣ技法に従ってメッセージを暗号化することによりシークレットS_i を、

【数１】

$$S_i = MAC_{part2(I_i^j)}(message)$$

として生成する。商人５０４との取引の完了により、ユーザ５０２は、part１（I_i^j），S_i，message，$E_{PKi}(C_i)$ のパラメータを商人５０４に送る。これらのパラメータの受け取りにより、商人５０４は、ユーザ５０２により注文されたアイテムを含むパッケージ５１０に対するラベル５０８を用意し、パッケージ５１０を配送業者５０６へ送る。

【００７２】上述したように、ユーザ５０２により商人５０４に送られるパラメータは、パッケージラベル５０８上に好都合に符号化されるには長すぎる可能性があり、パラメータのいくつかは、破線５３０により図５中に示されたように別の方法で（例えば、電子的に）、商人５０４により配送業者５０６へ送信され得る。望ましくは、ラベル５０８は、識別子 part１（I_i^j）を含み、その識別子に関連づけられた他のパラメータ、即ち S_i，message，$E_{PKi}(C_i)$ は、配送業者に電子的に送信される。

【００７３】パッケージ５１０の受け取りにより、配送業者５０６は、ラベル５０８上にある part１（I_i^j）についてデータベースサーチを行う。発見されると、配送業者５０６は、データベース記録から関連する part２（I_i^j）および商人５０４から電子的に受信されたmessage を取り、シークレット

【数２】

$$S_i = MAC_{part2(I_i^j)}(message)$$

を演算する。演算されたシークレットS_i が商人５０４から電子的に受信されたシークレットS_i と一致する場合、配送業者５０６は、ユーザ５０２がmessage中で特定された価格を支払うことに同意したに違いないと決定する。これは、そうでない場合、商人５０４は、配送業者５０６により演算されたシークレットS_iに一致するシークレットS_iを演算することはできなかったからである。

【００７４】この場合において、配送業者５０６は、商人５０４に、メッセージ中に特定された額を支払い、パッケージ５１０をユーザに配達し、ユーザ５０２に、配送料、配送業者が商人に支払った額、プラス支払いを取り扱うための適切な取引量を課金することができる。演算されたシークレットS_i が商人５０４から受け取ったシークレットS_i と一致する場合、ユーザ５０２は、支払いをすることに同意したことを否定できない。

【００７５】演算されたシークレットS_iが、商人５０４から受け取ったシークレットS_iと一致しない場合、問題があり、適切な例外処理が行われる。パッケージ５１０の受け取りにより、配送業者５０６がデータベース５１２中に part１(I_i^j) を見つけることができない場合、上述した外挿技法が使用され得る。

【００７６】以上の詳細な説明は、例示的なものと理解されるべきであり、限定的ではなく、ここに開示された発明の範囲は、詳細な説明により決定されるべきでなく、特許法により許容される範囲に従って解釈される特許請求の範囲から解釈されなければならない。ここに示された実施形態は、本発明の原理を単に例示したものであり、様々な修正が、当業者により本発明の範囲および精神から離れることなしになされ得る。例えば、送られるパラメータ、およびそのようなパラメータの暗号化に対する様々な修正および変形が、当業者にとって容易に明らかとなるであろう。例えば、ユーザは、ユーザの識別子を表すｉの暗号化された値および／または配送業者に渡された場合、データベースルックアップの性能を改良し得る他の暗号化されたパラメータを商人に渡すことができる。

【００７７】

【発明の効果】以上説明したように、本発明によれば、エレクトロニックコマースにおけるリンク可能でない匿名性配達技法を提供することができる。

【００７８】特許請求の範囲の発明の要件の後に括弧で記載した番号がある場合は本発明の一実施例の態様関係を示すものであって、本発明の範囲を限定するものと解釈してはならない。

【図面の簡単な説明】

【図１】本発明の一実施形態を示すために使用されるエレメントの構成を示す図。

【図２】本発明の別の実施形態を示すために使用されるエレメントの構成を示す図。

【図３】本発明の実施形態によるデータベース記録の内容およびデータベース情報の外挿を示す図。

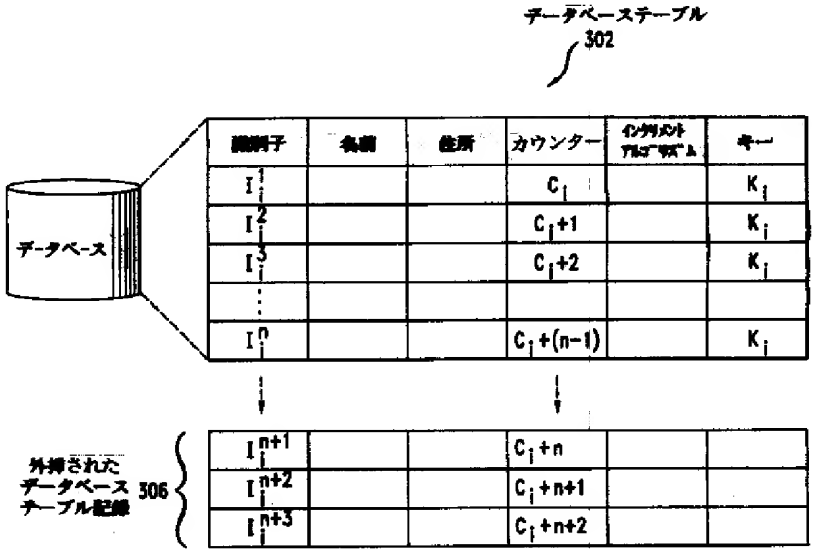
【図４】本発明の別の実施形態を示すために使用されるエレメントの構成を示す図。

【図５】支払い技法が配達技法に結合される本発明の一実施形態を示すために使用されるエレメントの構成を示す図。

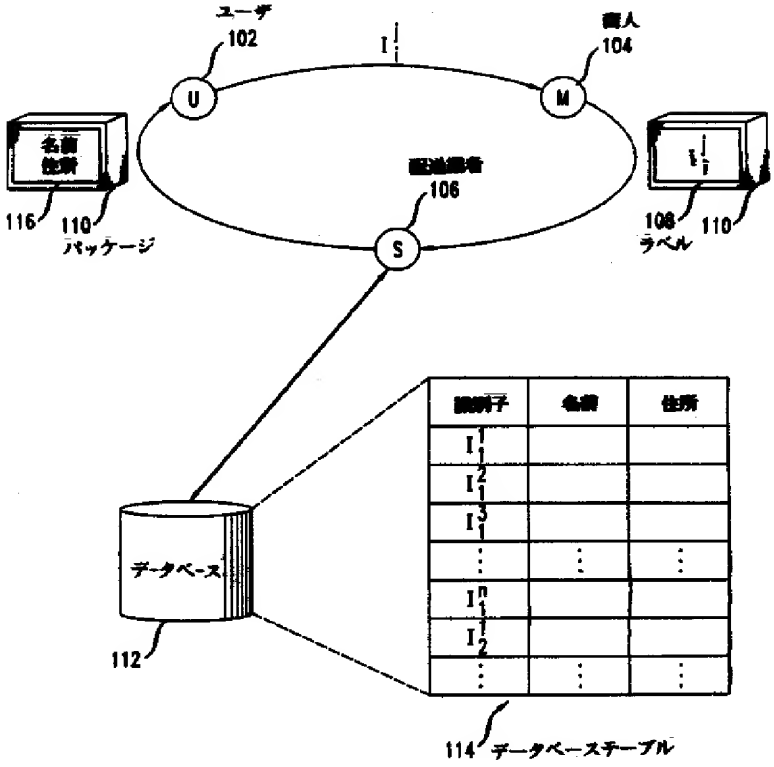
【符号の説明】

１０２，２０２，４０２，５０２　ユーザ
１０４，２０４，４０４，５０４　商人
１０６，２０６，４０６，５０６　配送業者
１０８，２０８，４０８，５０８　ラベル
１１０，２１０，４１０，５１０　パッケージ
１１２，２１２，４１２，５１２　データベース
１１４，２１４，４１４，５１４　データベーステーブル

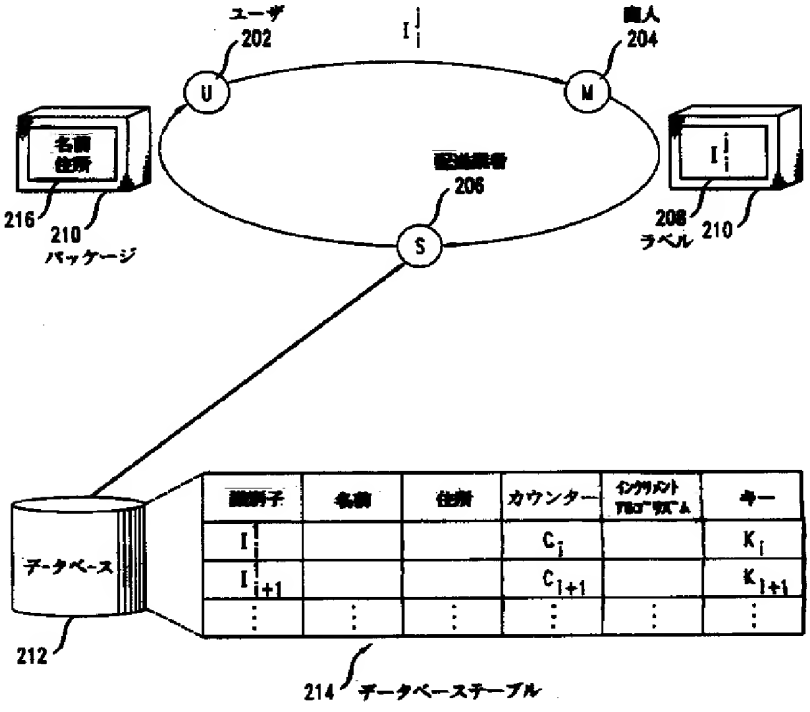
【図３】



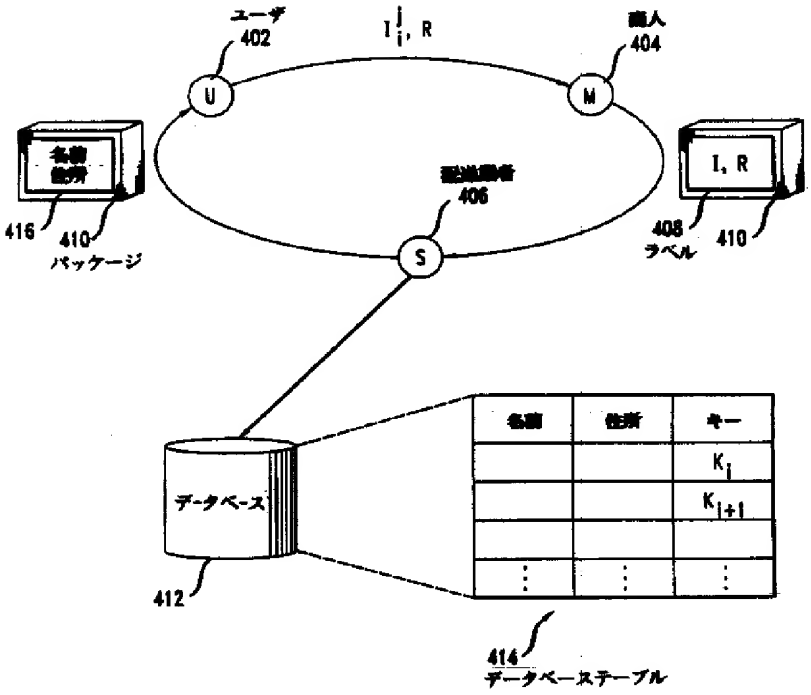
【図１】


ユーザ
102
商人
104
U
M
S
106
名前
住所
116
110
パッケージ
ラベル
108
110
データベース
112
識別子
名前
住所
114
データベーステーブル

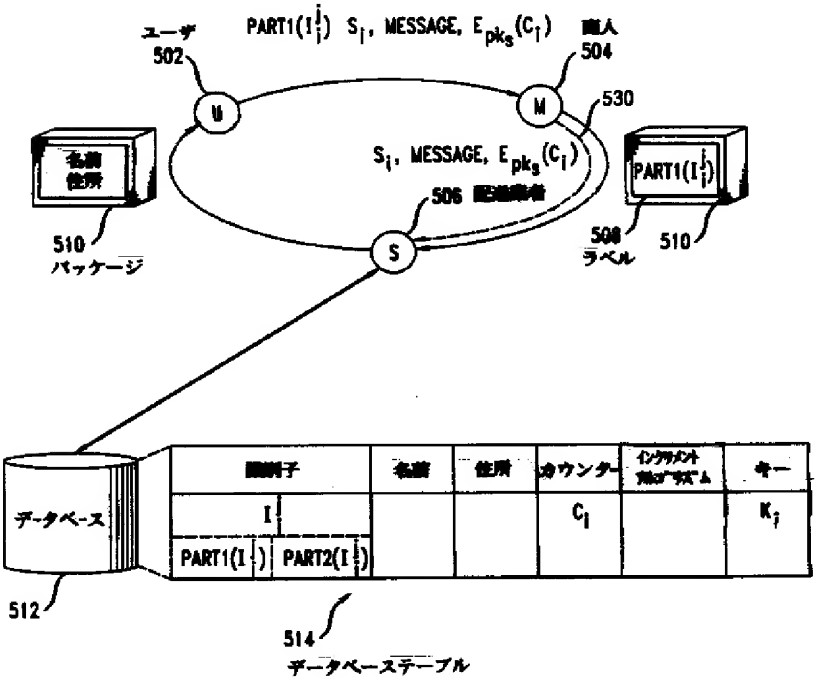
【図２】


ユーザ
202
商人
204
U
M
S
206
名前
住所
216
210
パッケージ
ラベル
208
210
データベース
212
識別子
名前
住所
カウンター
インクリメント
キー
214
データベーステーブル

【図4】


ユーザ
402
I_i^j, R
商人
404
U
M
名前
住所
I, R
経由機構
406
S
416
410
パッケージ
408
ラベル
410
データベース
412
名前
住所
キー
K_I
K_{I+1}
414
データベーステーブル

【図5】


ユーザ
502
PART1(I_i^j) S_I, MESSAGE, $E_{pk_S}(C_I)$
商人
504
U
M
530
名前
住所
S_I, MESSAGE, $E_{pk_S}(C_I)$
PART1(I_i^j)
506
S
510
パッケージ
508
ラベル
510
データベース
識別子
名前
住所
カウンター
インクリメント
ルックアップ
キー
I
PART1(I_i^j)
PART2(I_i^j)
C_I
K_I
512
514
データベーステーブル

フロントページの続き

(71)出願人 596077259
600 Mountain Avenue, Murray Hill, New Jersey 07974-0636U. S. A.
(72)発明者 ビョーン エム ジャコブソン
アメリカ合衆国、07030 ニュージャージー州、ホウボウカン、ガーデン ストリート 1203
(72)発明者 マイケル ケンドリック ライター
アメリカ合衆国、08869 ニュージャージー州、ラリタン、ブルーバード ウェイ 4
(72)発明者 アブラハム シルバーシャッツ
アメリカ合衆国、07059 ニュージャージー州、ウォラン、ウルフ ヒル ドライブ 48